SYSTEM AND METHOD FOR CUSTOMER MANAGEMENT OF THIRD PARTY VIRTUAL ROUTERS

Field

5   The present invention relates generally to computer network routers, and more particularly to systems and methods of customer management of routers provided by third parties.

Related Files

10   This application is related to the following copending and coassigned applications:

"SYSTEM AND METHOD FOR MANAGING AND PROVISIONING VIRTUAL ROUTERS", serial number _____, <Attorney Docket 1384.009>,

"SYSTEM AND METHOD FOR MANAGING ROUTER METADATA", serial number _____, <Attorney Docket 1384.011>,

15   and to two provisional applications each titled "SYSTEMS AND METHOD FOR DELIVERING INTERNETWORKING SERVICES" <Attorney Dockets 1384.012PRV AND 1384.013PRV>;

all of which are hereby incorporated herein by reference for all purposes.

Background

The use of networks, including the Internet continues to grow at ever increasing rates. As a result, there is increasing demand for network resources, including those provided by service providers such as Internet Service Providers (ISPs). ISPs typically provide the

5   hardware and software that allow their subscribers to access the network. Today's network based service providers encounter one major problem. Every change to the customer's needs turns into a change request or a work order for the service provider. Since the service provider has to get involved for every change and also has to spend manpower for every change, this process is expensive and time consuming. Also, for the end user, the turn around time for

10   getting a service change implemented is long.

Some Customer Network Management Systems have been deployed by service providers, which merely give a "view only" model for the network, with billing and network performance/status information. These systems do not even remotely address the configuration change problem stated above.

15   As a result, there is a need in the art for the present invention.

Summary

The above-mentioned shortcomings, disadvantages and problems are addressed by the present invention, which will be understood by reading and studying the following

20   specification.

To enable ISPs to deliver services using service processing switches, systems and methods are provided that make provisioning network resources, including Virtual Private Networks (VPNs) very easy. The systems and methods described reduce the resources required to manage a VPN network by allowing a subscriber to manage and control the

25   resources allocated to the subscriber. For example, it is possible for ISPs to provision VPNs for hundreds, or even thousands of subscribers, each with a variety of services. Once resources have been allocated, the subscriber can manage the resources without the need for the service provider to get involved in every case.

2

In one embodiment, a computerized system for providing subscriber control of network parameters includes a service processing switch having a plurality of network resources; a service provider management server communicably coupled to the service processing switch and operable to configure the plurality of network resources. The

5　configuration includes an allocation of a subset of the network resources to a subscribing enterprise. A subscriber management server is communicably coupled to the service provider management system and is operable to further configure the subset of the network resources. The system also includes a subscriber management client communicably coupled to the subscriber management server. The client is operable to issue configuration requests to the

10　subscriber management server.

The present invention describes systems, clients, servers, methods, and computer-readable media of varying scope. In addition to the aspects and advantages of the present invention described in this summary, further aspects and advantages of the invention will become apparent by reference to the drawings and by reading the detailed description that

15　follows.

Brief Description Of The Drawings

FIG. 1 is a block diagram of the hardware and operating environment in which different embodiments of the invention can be practiced;

20　FIG. 2 is a diagram illustrating an exemplary software environment according to embodiments of the invention;

FIG. 3 is a diagram illustrating an exemplary user interface screen according to an embodiment of the invention; and

FIG. 4 is a flowchart illustrating a method for configuring according to an embodiment of the

25　invention.

Detailed Description

In the following detailed description of exemplary embodiments of the invention,

3

reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific exemplary embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized

5   and that logical, mechanical, electrical and other changes may be made without departing from the scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense.

In the Figures, the same reference number is used throughout to refer to an identical component which appears in multiple Figures. Signals and connections may be referred to by

10   the same reference number or label, and the actual meaning will be clear from its use in the context of the description.

The detailed description is divided into multiple sections. In the first section the hardware and operating environment of different embodiments of the invention is described. In the second section, the software environment of varying embodiments of the invention is

15   described. In the final section, a conclusion is provided.

Hardware and Operating Environment

FIG. 1 is a diagram of the hardware and operating environment in conjunction with

20   which embodiments of the invention may be practiced. The description of FIG. 1 is intended to provide a brief, general description of suitable computer routing hardware and a suitable computing environment in conjunction with which the invention may be implemented. Although not required, the invention is described in the general context of computer-executable instructions, such as program modules, being executed by a computer, such as a

25   personal computer or a server computer. Generally, program modules include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types.

As shown in FIG. 1, the system 100 includes a service processing switch 110, access routers 104, service management system 118, and subscriber management system client 106.

4

In some embodiments, service processing switch 110 provides switching, routing and computing resources that can be allocated by a service provider to customers. In one embodiment, the service processing switch 110 is the IPSX 9000 service processing switch from CoSine Communications, Inc. However, the invention is not limited to any particular

5   switch, router or service processing hardware.

Service processing switch can contain one or more blades 112. In some embodiments of the invention, blades 112 have a type associated with them. Examples of blade types include, processing functions such as network blades, control blades, trunk blades, and processor blades. Network blades provide interfaces to different types of networks. Control

10   blades provide system management and accounting functions to the service processing system 110. Trunk blades provide access to high speed trunk networks. Processor blades provide general purpose computer processors that in some embodiments of the invention provide firewall, intrusion detection, or directory services. Blades are communicably coupled to one another, in one embodiment a packet ring is used to communicably couple the blades.

15   In some embodiments, each of blades 112 includes one more processing elements 114. Processing elements 114 include CPU and memory that provide computing resources for the blade. The invention is not limited to any particular number of processing elements on a blade, nor is the invention limited to any particular number of blades in a service processing switch 110.

20   Service processing system 110 is typically communicably coupled to a network 116, for example the Internet. Network 116 can also be a Wide Area Network (WAN), a Local Area Network (LAN), or a private network.

Service processing system 110 is also typically communicably coupled to a plurality of customer networks 102 via customer access routers 104.

25   Service management system 118 hosts software that is used to configure and control the operation of service processing switch 110. In one embodiment of the invention, the service management system is a SPARC system available from Sun Microsystems, Inc. running the InVision product from CoSine Communications, Inc. Service management system 118 can be used to allocate resources within service processing switch 110 to various

customers. In one embodiment of the invention, service management system 118 communicates with service processing switch 110 using the Simple Network Management Protocol (SNMP). Further details on the operation of service management system 118 are provided in U.S. Patent Application serial number _____, entitled "SYSTEM AND

5   METHOD FOR MANAGING AND PROVISIONING VIRTUAL ROUTERS", previously incorporated by reference.

Subscriber management system client 106 hosts software that configures and controls the resources within service processing switch 110 that have been allocated to the particular customer. The operation of software running on subscriber management system client 106

10   will be described in further detail in the sections that follow.

Subscriber management system server 120 hosts software that responds to requests from subscriber management system client 106. A logical connection between client 106 and server 120 is indicated by the dashed line. The operation of subscriber management systems server 120 will be described in further detail below.

15   Those skilled in the art will appreciate that the invention may be practiced with other routing system hardware configurations besides those described above.

Software Environment

The embodiments of the invention include a software environment of systems and

20   methods that provide a mechanism for subscribers to manage the services provided to them by a third party network service provider such as an Internet Service Provider (ISP). This includes managing subscriber related aspects of VPN (Virtual Private Networks) and VRs (Virtual Routers) and other resources allocated by to the subscriber within a service processing switch. Generally speaking, the embodiments of the invention include policy-

25   based mechanism for network service management. Thus a service provider, such as an ISP managing a service processing switch can create and generate tunnels, routing, and other service configurations for VPNs (Virtual Private Networks). These VPNs use resources within switch 110 such as blades and processing elements that are allocated by a service provider to one or more subscribers, who then can configure those elements allocated to them.

6

Configuration from the subscriber's perspective can be driven based on profiles. One subscriber cannot view, modify, or create configurations involving the resources allocated to a different subscriber.

FIG. 2 provides an illustration of a subscriber configuration management system as used in various embodiments of the invention to provide subscriber management of network services provided by a third party. As illustrated, the system includes a subscriber management server 210, a service provider management system 220, and a subscriber management client 202.

Subscriber management client 202 comprises software that a subscriber uses to create, view, and modify the configuration network resources (typically virtual network resources) that have been allocated to the subscriber by a service provider. In one embodiment, the client 202 is browser based and works with web browsers such as Internet Explorer and Netscape. However, the invention is not limited to web browsers, and client component 202 can be applications software that provides a user interface for creating viewing, and modifying configuration parameters for resources within a virtual network.

Subscriber management server 210 receives requests from subscriber management client 202. In one embodiment, subscriber management server is provided as part of the InGage software system from CoSine Communication, Inc. In one embodiment of the invention, the server 210 is includes web server software and communicates with client 202 using a secure Internet protocol such as the HTTPS (HyperText Transfer Secure) protocol. Using a secure Internet protocol is desirable, because it allows users around the world to securely view and manage network service configurations. The subscriber management server 210 hosts and runs programs which expose specific functionality to the enterprise customers (i.e. subscribers) that the service providers want to provide to the enterprise customers. In one embodiment of the invention, the subscriber management server includes software programs that provide the following functions:

- Ability to add and remove enterprise users of the enterprise's VPN(s).
- Exposing limited firewall settings to the enterprise customer so that they can modify specific components of the firewall settings directly.

- Monitor the state of the subscriber's enterprise VPN(s).

- Provide Reports

- Maintain Audit Trail information, including:

    o Login attempts

    o Reports/Pages accessed

    o Logs of all user addition/deletion and user privilege modifications

    o Logs of all enterprise policy changes

- Maintain Usage Accounting, including:

    o Number of users

    o Resources usage per enterprise

    o Resources usage per user

    o Concurrent sessions

It should be noted that the above described functions can be included in differing combinations in the various embodiments of the invention, and the invention is not limited to any particular combination of the above described functions.

Subscriber management server 210 includes a subscriber access control component 212. Subscriber access control component 212 operates to provide a layer of security in addition to that provided through the HTTPS protocol. In some embodiments of the invention, various privilege levels are provided to users. In one embodiment, three levels of user privileges are provided:

1. ISP Administrator
2. Enterprise Administrator
3. Enterprise User

ISP Administrator is a privilege that can be granted to the administrators of the subscriber management system, who act as "super-users" of the system. When subscriber management functionality is to be provided to an enterprise, an ISP Administrator can login to the subscriber management system and create the users for the enterprise. Typically, the ISP Administrator can just create one user for the enterprise with the role "Enterprise

8

Administrator". The ISP Administrator also has privileges to use any enterprise VPN and create/delete/modify any user for any enterprise VPN.

An Enterprise Administrator is a role that has a defined scope within a given enterprise. i.e., every enterprise customer can have one or more Enterprise Administrators. An

5   enterprise administrator is a role that acts as a super-user for all the subscriber management related functionality for a particular enterprise's VPN or set of VPNs. An Enterprise Administrator can create other enterprise users within the subscribing enterprise's VPN. The role also allows for creating/modifying/deleting other Enterprise Users for the VPN, and use of any functionality exposed for the VPN through the subscriber management system. In

10   addition, an Enterprise Administrator can modify any configuration or policy entries for the enterprise. Further, Enterprise Administrators can view/edit/add/delete packet filter and firewall policies and view/edit/add/delete NAT (Network Address Translation) policies for one or more sites belonging to their enterprise

An Enterprise User is a role that can be created within the scope of a subscribing

15   enterprise's VPN. Also, various access levels can be given for an enterprise user. In some embodiments, Enterprise User's are limited to monitoring functions, that is, they can view VPN statistics and configurations, but cannot modify them. For example, an Enterprise User can view packet filter and firewall policies for one or more sites belonging to their enterprise. In addition, Enterprise Users can view NAT (Network Address Translation) policies for one

20   or more sites belonging to their enterprise. In other alternative embodiments, subscriber management functionality such as Firewall Monitoring, Network Monitoring, Firewall Configuration etc. can be permitted or denied for each individual enterprise user. Similarly, if an enterprise VPN is connecting various enterprise sites, an enterprise user can be configured to have privileges only for those sites that the user has permissions to.

25   As noted above, the subscriber management system includes the ability to monitor the configuration and status network resources allocated to a subscriber. Included in the monitoring function is the ability to perform the following:

9

- Provide a list of all the ports allocated to a particular enterprise customer with their status. In one embodiment, the list includes:

  - Site Name – the location of the enterprise customer's site connected to this port
  - Port Type – type of port such as Ethernet, DS3, OC-3 etc. It should also display encapsulation details such as the link is running PPP, HDLC or Frame Relay.
  - Port Status – the status of the port/interface i.e., up/down
  - Features – should list all the features available for this site, such as firewall, NAT, etc. It should also indicate the status of these features, i.e., enabled or disabled.

- Provide a list of all the tunnels created for the particular enterprise customer with their status. In one embodiment, each entry includes:

  - Tunnel Endpoint1 Site Name – the location of the enterprise customer's site connected to one end of the tunnel
  - Tunnel Endpoint2 Site Name – the location of the enterprise customer's site connected to the other end of the tunnel
  - Features or Type of Tunnel – should indicate Manual IPSec, IKE etc
  - Status – the status of the tunnel i.e., up/down

- Provide a graphical topology of the customer's VPN. In one embodiment, the graphical topology shows the customer sites and the connecting tunnels

As noted above, some embodiments of the invention provide reporting capability. Included in the reports generated by the subscriber management system are performance reports for ports allocated to the subscriber. In one embodiment of the invention, these reports include:

- Total Packets (packets/sec)
- Total Bytes (bytes/sec)
- Total Discards In & Out (packets/sec)
- Total Errors (errors/sec)
- Availability

In addition, performance reports related to tunnels created for the enterprise can be generated. In one embodiment, these reports include the following:

- Total Packets (packets/sec)
- Total Bytes (bytes/sec)
- Total Discards In & Out (packets/sec)
- Total Errors (errors/sec)
- Latency

Service provider management server 220 is communicably coupled to subscriber management server 210, and operates to service requests received from subscriber management server 210 to perform the functions described above. In one embodiment, service provider management system is the InVision system available from CoSine Communications, Inc. Service provider management system 220 controls the network and network elements in the service provider's network. In some embodiments, subscriber management system 210 never directly communicates with the network elements. Instead, it uses the interfaces exposed by the service provider management system 220. Service provider management system 220, in turn, performs the operations on subscriber management server's behalf on the network.

In some embodiments of the invention, service provider management server 220 includes provider access control component 222 and choking component 224. Provider access control component 222 provides security using an access control mechanism. The access control mechanism provides user level access control. In one embodiment of the invention a special user is created to represent subscribers. In one embodiment, the user is called "InGage". This user is only exposed only the functionality required by subscriber management systems. In some embodiments, during its startup procedures, subscriber management server 210, creates a user session with the service provider management system by logging in as "InGage" and providing the appropriate password. This level of security

11

ensures that only the kind of functions exposed to the subscriber management system can be used by a hacker who can hack into the service provider management system 220 directly.

Choking component 224 provides a mechanism to ensure that not more than a configurable active subscriber management requests can be submitted to service provider management system concurrently. If the total number of requests submitted by subscriber management server 210 ever exceeds the maximum allowed, the requests are queued so that a flood of subscriber management requests cannot bring the service provider management system or the network down.

An exemplary user interface screen 302 is illustrated in FIG. 3. As shown screen 302 includes a VPN list 308, router-level firewall rules configuration 304, and Internet interface firewall rules 306. VPN list 308 provides a list of VPNs and nodes within the VPN that are currently configured for the subscribing enterprise. As a user selects a VPN or a VPN node from the list, the rules associated with the VPN or node are displayed. In one embodiment, the router level rules 304 include a rule priority, a source and destination address associated with the rules, an action (i.e. permit, deny etc.), the proxy type, the policy name for the policy to be applied, the protocol, the port, and sync flag.

Internet interface firewall rules 306 in one embodiment include source and destination addresses, action to be taken (i.e. permit, deny), the protocol, the source and destination ports, the TCP status of the connection, the direction of packets (i.e. inbound or outbound) and the sync flag.

This section has described a system level overview of the software according to various embodiments of the invention that provide for subscriber configuration of virtual network resources allocated by a service provider. It should be noted that while a multiple tier system has been presented, other configurations are possible and within the scope of the invention. For example, the functionality of the subscriber management server 210 and the service provider management server 220 could reside on the same hardware. In addition, multiple instances of subscriber server 210 can exist in order to provide scalability to the system, thereby allowing a service provider to scale up the number of users who can access

the system by adding more server machines to the network, which can seamlessly share the load to ensure that all the subscribing users are serviced uniformly.

Methods For Performing Profile-Based Routing Configuration

5

In the previous section, a system level overviews of the operation of exemplary embodiments of the invention were described. In this section, the particular methods of the invention performed by an operating environment executing an exemplary embodiment are described by reference to a flowchart shown in FIG. 4. The methods to be performed by the

10   operating environment constitute computer programs made up of computer-executable instructions. Describing the methods by reference to a flowchart enables one skilled in the art to develop such programs including such instructions to carry out the methods on suitable computers (the processor of the computer executing the instructions from computer-readable media). The method illustrated in FIG. 4 is inclusive of the acts required to be taken by an

15   operating environment executing an exemplary embodiment of the invention.

A method for configuring network resources 400 begins when network resources are allocated to a subscribing enterprise. The network resources include processing elements, virtual routers, virtual private networks, network interfaces, virtual interfaces and network ports (block 402).

20   After resources have been allocated, a subscriber management system receives a request related to the allocated resources (block 404). Typically the request will come from a browser application. The request can be to view a configuration of network resources, or the request can be to modify the configuration.

Next, the request is forwarded to a service provider management system (block 406).

25   The service provider management system performs validation checks to ensure that the request is for resources allocated to the subscriber. If the request is valid, the service provider management system executes the request (block 408). In some embodiments, the service

13

provider management system uses SNMP (Simple Network Management Protocols) to cause a service providing switch to be updated with the configuration request.

5

Conclusion

Systems and methods for providing a subscriber the ability to configure and maintain virtual router resources allocated by an service provider are disclosed. The embodiments of the invention provide advantages over previous systems. For example, the embodiments of the
10 invention provide a mechanism for a subscriber to configure services provided by a network service provider with zero software maintenance from the subscriber's point of view. The subscriber does not have to install, update or maintain any software element in the enterprise site for easily and rapidly generating configuration information for large numbers of virtual routers and virtual private networks based on profiles. In addition, the subscriber maintains a
15 level of control over the network resources they have been allocated, thereby reducing or eliminating the mistrust many subscribers have due to the outsourcing of network service to service providers. Furthermore, subscribers obtain views of their service, and updates on network performance that can be compared with service level commitments. In addition, subscribers can adjust various network parameters without having to rely on or wait for the
20 network service provider to perform the change. Conversely, the network service provider is not overwhelmed with the many change requests that each subscriber invariably makes.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to
25 achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention.

The terminology used in this application is meant to include all of these environments. It is to be understood that the above description is intended to be illustrative, and not restrictive. Many other embodiments will be apparent to those of skill in the art upon

14

reviewing the above description. Therefore, it is manifestly intended that this invention be limited only by the following claims and equivalents thereof.